Fontaine-Mazur conjecture and p-adic Galois representations

Exercises

13th June 2014

In this series of exercises we construct the Witt rings of perfect rings of characteristic p. Let A be a commutative ring with 1 in which $p = \underbrace{1 + \cdots + 1}_{p} \in A$ is not a zero divisor and the natural map $A \to \varprojlim_n A/p^n A$ is an isomorphism (ie. A is *p-adically complete*). Further suppose that $R := A/pA$ is a *perfect ring of characteristic* p, that is the p-power Frobenius is bijective: for all $x \in R$ there exists uniquely a $y := x^{p^{-1}} \in R$ with $x = y^p$. These rings A are called *strict p-rings*. For example $A = \mathbb{Z}_p$ is a strict p-ring.

1. Show that on fields k of characteristic p the Frobenius is always injective and it is surjective if and only if none of the irreducible polynomials over k have a multiple root.

2. Show that a ring R of characteristic p (ie. commutative and $\underbrace{1 + \cdots + 1}_{p} = 0$) is reduced (ie. contains no nilpotent elements) if the Frobenius is injective.

3. Let A be a strict p-ring with $R = A/pA$ perfect of characteristic p. For any $x \in R$ denote by $\hat{x}$ an arbitrary lift of x to A (ie. $x = \hat{x} + pA$). We choose once and for all such a lift for each $x \in R$. Show that the limit $[x] := \lim_{n\to\infty}(\widehat{x^{p^{-n}}})^{p^n}$ exists in A in the p-adic topology. Moreover, verify that $[xy] = [x][y]$. The element $[x] \in A$ is called the multiplicative (or Teichmüller) representative of x.

4. Show that in a strict p-ring A any element $x \in A$ can be uniquely written in the form

$$x = \sum_{i=0}^{\infty} p^i [x_i]$$

where $[x_i] \in A$ are multiplicative representatives of elements $x_i \in R$. Moreover, any sum like that converges in the p-adic topology.

Let R be a perfect ring of characteristic p. Our goal is to construct a strict p-ring $W(R)$ such that $R \cong W(R)/pW(R)$. Further, we would like to do this functorially in R. Such a $W(R)$ will be unique up to a unique isomorphism and will be called the Witt ring of R. The elements of $W(R)$ will have the form $\sum_{i=0}^{\infty} p^i [x_i]$ with $x_i \in R$. Here $[x_i]$ denotes a formal multiplicative representative of x_i in $W(R)$. In order to define the addition and multiplication on these formal power series we first need to construct the Witt ring of a free perfect ring of characteristic p on countably many generators. Let $X_0, X_1, \ldots, Y_0, Y_1, \ldots$ be formal variables. Moreover, let $X_i^{p^{-n}}$ and $Y_i^{p^{-n}}$ denote a formal p^nth root of these variables. Further let

$$\begin{aligned} \mathbb{Z}_p[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}} \mid i \geq 0] &:= \bigcup_n \mathbb{Z}_p[X_i^{p^{-n}}, Y_i^{p^{-n}} \mid i \geq 0] \ ; \\ S &:= \varprojlim_n \mathbb{Z}_p[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}} \mid i \geq 0]/(p^n) \ . \end{aligned}$$

5. Show that S is a strict p-ring. Therefore there exist polynomials $S_i, P_i \in S/pS = \mathbb{F}_p[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}} \mid i \geq 0]$ for which

$$\begin{aligned} \left(\sum_{i=0}^{\infty} p^i X_i\right) + \left(\sum_{i=0}^{\infty} p^i Y_i\right) &= \sum_{i=0}^{\infty} p^i [S_i] \\ \left(\sum_{i=0}^{\infty} p^i X_i\right) \left(\sum_{i=0}^{\infty} p^i Y_i\right) &= \sum_{i=0}^{\infty} p^i [P_i] \ . \end{aligned}$$

6. Determine the polynomials $S_0, S_1, P_0, P_1 \in \mathbb{F}_p[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}} \mid i \geq 0]$.

7. Let R be a perfect ring of characteristic p and put $W(R) = \{r = (r_0, r_1, \ldots) \mid r_i \in R, i \geq 0\} = R^{\mathbb{N}}$ as a set. Consider the following operations on $W(R)$: $(r+s)_n := S_n(r_0, r_1, \ldots, s_0, s_1, \ldots)$ and $(rs)_n := P_n(r_0, r_1, \ldots, s_0, s_1, \ldots)$. Show that this equips the set $W(R)$ with a structure of a strict p-ring.

8. Prove the following universal property of $W(R)$: if A is any strict p-ring and $\varphi \colon R \to A/pA$ is a ring homomorphism then there exists a unique homomorphism $\tilde{\varphi} \colon W(R) \to A$ lifting φ, ie. φ equals $\tilde{\varphi}$ modulo p). In particular, W is a functor from the category of perfect rings of characteristic p to the category of strict p-rings. Remark: $\mathrm{Frob}_p \colon R \to R$ can also be lifted to $W(R)$. We call this Frobenius-lift.

9. Show that the functors $R \mapsto W(R)$ and $A \mapsto A/pA$ are quasi-inverse equivalences of categories between the category of strict p-rings and the category of perfect rings of characteristic p.

---

10. Show that the field $\mathbb{C}_p := \widehat{\overline{\mathbb{Q}_p}}$ is algebraically closed. (Here $\bar{\cdot}$ stands for the algebraic closure and $\hat{\cdot}$ stands for the completion with respect to the p-adic absolute value.)

11. For a finite extension $K/\mathbb{Q}_p$ (inside $\overline{\mathbb{Q}_p}$) denote by $G_K = \mathrm{Gal}(\overline{\mathbb{Q}_p}/K)$ its absolute Galois group. Since the action of G_K is continuous (isometric) on $\overline{\mathbb{Q}_p}$ it extends to the completion $\mathbb{C}_p$. Show that $\mathbb{C}_p^{G_K} = K$, ie. there are no transcendental invariants.

12. (Hilbert 90 for GL_n) Show that for any finite Galois extension L/K of fields we have

$$H^1(\mathrm{Gal}(L/K), \mathrm{GL}_n(L)) = \{1\} \ .$$

Note that for $n > 1$ this is just a pointed set, not a group. Recall that the nonabelian group cohomology is defined as follows: if the group G acts on the group A via automorphisms then $H^1(G, A)$ is the set of equivalence classes of 1-cocycles: a 1-cocycle is a map $\varphi\colon G \to A$ with the property that $\varphi(gh) = \varphi(g)\cdot(g\varphi(h))$. Moreover, φ is equivalent to φ' if there exists an $a \in A$ such that for all $g \in G$ we have $a\varphi'(g) = \varphi(g)\cdot(ga)$. The distinguished element of the set $H^1(G, A)$ is the equivalence class of the constant 1 map.

13. (Thm. Ax–Sen–Tate) Prove that for any closed subgroup $H \le G_K$ we have $\mathbb{C}_p^H = \widehat{L}$ where $L = \overline{\mathbb{Q}_p}^H$.

The following exercises are meant to be done after the course.

14. Let Λ be a finitely generated $\mathbb{Z}_p$-module equipped with a continuous representation by $G_K = \mathrm{Gal}(\overline{K}/K)$ for the fraction field K of a complete discrete valuation ring. Let $\rho\colon G_K \to \mathrm{Aut}_{\mathbb{Z}_p}(\Lambda)$ be the associated homomorphism. Prove that $\mathrm{Ker}\rho$ is a closed normal subgroup in G_K, and let K_∞ be the corresponding fixed field; we call it the splitting field of ρ. In case ρ is the Tate module representation of an elliptic curve E over F with $\mathrm{char}(K) \neq p$, prove that the splitting field of ρ is the field $K(E[p^\infty])$ generated by the coordinates of the p-power torsion points.

---

15. Let E be an elliptic curve over K with split multiplicative reduction, and consider the representation space $V_p(E) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(E) \in \mathrm{Rep}_{\mathbb{Q}_p}(G_K)$. The theory of Tate curves provides an exact sequence

$$0 \to \mathbb{Q}_p(1) \to V_p(E) \to \mathbb{Q}_p \to 0$$

that is non-split in $\mathrm{Rep}_{\mathbb{Q}_p}(G_{K'})$ for all finite extensions K'/K inside of $\overline{K}$. Show that the exact sequence

$$0 \to \overline{K}(1) \to \overline{K} \otimes_{\mathbb{Q}_p} V_p(E) \to \overline{K} \to 0$$

is not split in the category $\mathrm{Rep}_{\overline{K}}(G_K)$ of semilinear representations of G_K on $\overline{K}$-vector spaces either. However, the exact sequence

$$0 \to \mathbb{C}_p(1) \to \mathbb{C}_p \otimes_{\mathbb{Q}_p} V_p(E) \to \mathbb{C}_p \to 0$$

splits in $\mathrm{Rep}_{\mathbb{C}_p}(G_K)$.

16. Let $\eta\colon G_K \to \mathbb{Z}_p^\times$ be a continuous character. Identify $H^1_{cont}(G_K, \mathbb{C}_p(\eta))$ with the set of isomorphism classes of extensions

$$0 \to \mathbb{C}_p(\eta) \to W \to \mathbb{C}_p \to 0$$

in $\mathrm{Rep}_{\mathbb{C}_p}(G_K)$ as follows: using the matrix description

$$\begin{pmatrix} \eta & * \\ 0 & 1 \end{pmatrix}$$

of such a W, the homomorphism property for the G_K-action on W says that the upper right entry function is a 1-cocycle on G_K with values in $\mathbb{C}_p(\eta)$, and changing the choice of $\mathbb{C}_p$-linear splitting changes this function by a 1-coboundary.

---

17. Let R be a discrete valuation ring with maximal ideal $\mathfrak{m}$ and residue field k, and let $A = \mathrm{Frac}(R)$. There is a natural structure of a filtered ring on A via $A^i = \mathfrak{m}^i$ for $i \in \mathbb{Z}$. In this case the associated graded ring $\mathrm{gr}^\bullet(A)$ is a k-algebra that is non-canonically isomorphic to a Laurent polynomial ring $k[t, 1/t]$ upon choosing a k-basis of $\mathfrak{m}/\mathfrak{m}^2$. Show that canonically $\mathrm{gr}^\bullet(A) \cong \mathrm{gr}^\bullet(\hat{A})$, where $\hat{A}$ denotes the fraction field of the completion $\hat{R}$ of R.

18. Let the ring R be $R := \varprojlim_{x \mapsto x^p} \mathcal{O}_{\mathbb{C}_p}/(p)$. Show that R has no zero divisiors and $\mathrm{Frac}(R)$ is an algebraically closed field of characteristic p.

19. Show that B_{dR}^+ is *not* $(\mathbb{Q}_p, G_K)$-regular.

20. Show that a 1-dimensional p-adic Galois-representation is deRham if and only if it is Hodge-Tate.

21. Show that a p-adic Galois representation V is deRham (resp. Hodge-Tate) if and only if all its Tate twists $V(r)$ are deRham (resp. Hodge-Tate).

22. Calculate explicitely $D_{cris}(\mathbb{Q}_p(r))$.

23. Calculate explicitely $D_{st}(V_p(E))$ where E is an elliptic curve over K with split multiplicative reduction (you may assume it is a Tate curve).